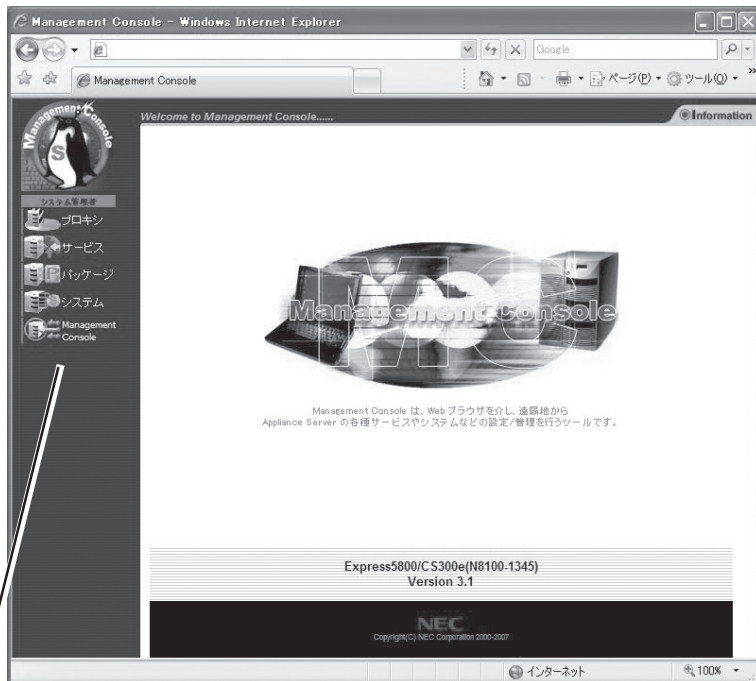
4 システムの管理

この章では、本装置で提供するサービスとWebベースの運用管理ツールである「Management Console」を利用した設定/管理について説明します。この「Management Console」からインターネットサービスに必要となるプロキシサーバを容易に管理することができます。

Management Consoleについて

ネットワーク上のクライアントマシンからWebブラウザを介して表示されるのが「Management Console」です。Management Consoleからシステムのさまざまな設定の変更や状態の確認ができます。

この章では、「管理者用」のManagement Consoleで利用できるさまざまなサービスの設定や確認、システムの操作方法を中心に説明します。

Management Console管理者用トップページ

ブラウザ上から項目（アイコン）をクリックすると、それぞれの設定画面に移動することができる。

【Management Consoleの画面構成】

■ システム管理者用トップページ

- プロキシ
- サービス
- パッケージ
- システム
- Management Console*

Management Consoleのセキュリティモード

Management Consoleでは、日常的な運用管理のセキュリティを確保するために、2つのセキュリティモードをサポートしています。

- **レベル1（パスワード）**

  パスワード認証による利用者チェックを行います。ただし、パスワードや設定情報は暗号化されません。

- **レベル2（パスワード + SSL）**

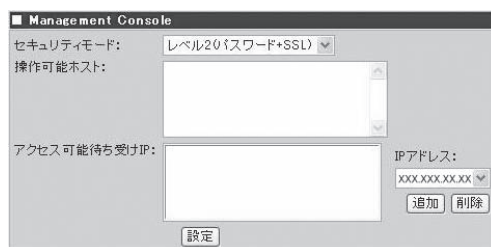
  パスワード認証に加えて、パスワードや設定情報をSSL（Secure Soket layer）で暗号化して送受信します。自己署名証明書を用いているため、「セキュリティ証明書は信頼する会社から発行されていません」という内容の警告ダイアログボックスが表示されます。

デフォルトの設定では、「レベル2」に設定されています。セキュリティレベルを変更する場合は、Management Console画面の［Management Console］アイコンをクリックして設定を変更してください。また、同画面で操作可能ホストを設定することにより、さらに高いレベルのセキュリティを保つことができます。

InternetExplorer7では、右図のようなエラー画面が表示される場合があります。「このサイトの閲覧を続行する」をクリックし、Management Console画面を開いてください。

システムの管理

アクセス可能待ち受けIP

本製品に割り当てられているIPアドレスの中から、Management Consoleのアクセスを許可するIPを指定します。例えばローカルIPとグローバルIPが割り当てられている場合、ローカルIPのみでアクセスを許可し、グローバルIPはアクセスを拒否する事で、本製品のセキュリティを高める事が可能です。リストボックスが空の場合は、すべてのIPでアクセスを受け付けます。

重要

- InternetExplorer7では、セキュリティ証明書のエラー画面が表示される場合があります。「このサイトの閲覧を続行する」をクリックし、Management Console画面を開いてください。
- 各画面の右上にある「ヘルプ」リンクをクリックすると、オンラインヘルプが表示されます。項目毎の説明、設定例などを記載していますので、ご覧ください。

Management Consoleへのアクセス方法

システム管理者は、Management Consoleを利用することにより、クライアント側のブラウザからネットワークを介してあらゆるサービスを簡単な操作で一元的に管理することができます。以下に各セキュリティモードにおけるアクセス手順を示します。

重要

- **Management Consoleへのアクセスには、プロキシを経由させないでください。**
- **インターネット側からManagement Consoleにアクセスする場合は、レベル2に設定してください。**
- **レベル2では、HTTPSプロトコル、ポート番号50453を使用します。**
- **Management Consoleへアクセスする場合にはブラウザのキャッシュ機能を使用しないようにしてください。**

レベル1の場合

1. クライアント側のブラウザを起動する。
2. URL入力欄に「http://<本装置に割り当てたIPアドレスまたはFQDN>:50090/」と入力する。
3. Management Console」画面で、[システム管理者ログイン]をクリックする。
4. ユーザー名とパスワードの入力を要求されたら、ユーザー名には「admin」、パスワードにはセットアップ時に指定した管理者パスワードを入力する。

レベル2の場合

1. クライアント側のブラウザを起動する。
2. URL入力欄に「https://<本装置に割り当てたIPアドレスまたはFQDN>:50453/」と入力する。
3. 警告ダイアログボックスが表示されたら、[はい]をクリックして進む。
4. [Management Console]画面で、[システム管理者ログイン]をクリックする。
5. ユーザー名とパスワードの入力を要求されたら、ユーザー名には「admin」、パスワードにはセットアップ時に指定した管理者パスワードを入力する。

Management Consoleにログインできたら、管理者用のトップページが表示されます。

重要

InternetExplorer7では、セキュリティ証明書のエラー画面が表示される場合があります。「このサイトの閲覧を続行する」をクリックし、Management Console画面を開いてください。

プロキシ

頻繁にアクセスするページをキャッシングすることにより、次回、同じページにアクセスした際に、ブラウザの表示時間を短縮します。
管理者は、Management Consoleから、有害なWebサイトなどへのアクセスの制限、不正なアクセスの制限などを設定することができます。
また、頻繁に参照されるWebページをシステムに自動的にダウンロードさせ、システム内に格納しておくための設定もできます。
これらの設定により、効率的なインターネットへのアクセスを実現します。

プロキシサーバ

プロキシサーバの起動状態を表示します。[再起動]をクリックするとプロキシサーバの再起動を行います(システムは再起動しません)。

スケジュールダウンロード

コンテンツを定期的にダウンロードしてキャッシュに格納するスケジュールダウンロードの状態を表示します。スケジュールダウンロードの使用を止める場合には、[一時停止]をクリックしてください。スケジュールダウンロードの再開は[起動]をクリックします。

基本設定

ブラウザなどからの要求を受け付けるIPアドレスやポート番号など、プロキシサーバを動作させるための基本的な設定をサーバ種別に応じて設定します。

重要

- **キャッシュサーバを登録、変更する場合には 必ず、[追加]、[編集]をクリックしてください。DNS設定やWebサーバ設定についても同様です。**
- **[設定]をクリックしないと、システムに反映されません。**

基本設定(リバースプロキシ)

[プロキシ]画面の[基本設定]でサーバ種別設定を「Reverse」と選ぶことによって表示される画面です。この画面では、システムをリバースモードで運用する際の設定ができます(システムをリバースモードで運用するには DNSサーバとの連携が必須です)。

■基本設定(リバースプロキシ)

サーバ種別設定	Reverse	
サーバの持続性	☑ サーバの持続性を有効にする	
DNS名チェック	☑ DNS名をチェックする	
キャッシュサーバ設定	xxx.xxx.xxx.xxx : 8080	キャッシュサーバアドレス xxx.xxx.xxx.xxx キャッシュサーバポート番号 [1-65535] 追加 編集 削除
ICPポート番号設定	ICPポート番号	ICP要求を受け付ける 3130 [1025-65535]
DNS設定		DNS名 追加 編集 削除
Webサーバ設定		Webサーバ名 ポート番号[1-65535] 追加 編集 削除

設定 戻る

重要

- **キャッシュサーバを登録、変更する場合には 必ず、[追加]、[編集] をクリックしてください。DNS設定やWebサーバ設定についても同様です。**
- **[設定]をクリックしないと、システムに反映されません。**
- **ReverseHTTPSとして運用される場合には、DNS名は1つしか設定しないでください。**
- **HTTPSのポート番号は、443で固定です。**
- **リバースプロキシが対応するプロトコルはHTTPとHTTPSです。**

セキュリティ設定

クライアントIPアドレス制限と、CONNECTトラフィック制限を行います。

重要

- **サーバ種別にReverseを設定している場合は、クライアントIPアドレス制限は無効となります。**
- **「クライアントIPアドレス制限」と「CONNECTトラフィック制限」と「アクセス制限」の制限処理の順番は以下の通りです。制限処理の順番によって設定が無効になる場合がありますので注意してください。**
  1. **クライアントIPアドレス制限**
  2. **CONNECTトラフィック制限**
  3. **アクセス制限**

親プロキシ設定

階層構造を形成する場合に親プロキシを設定することができます。
親プロキシの指定と、親プロキシの選択方法を設定します。

隣接プロキシ設定

階層構造を形成する場合にシステムの隣接プロキシを設定することができます。

隣接プロキシを設定すると、指定した隣接サーバの設定によっては、Web閲覧の際にページや画像が正しく表示されない場合があります。指定した隣接サーバの設定を確認し、設定し直すか、ここでの設定を削除してください(7章の「トラブルシューティング」も併せて参照してください)。

詳細設定

[プロキシ]画面の[詳細設定]でプロキシサーバとしての詳細な動作設定ができます。

アクセス制御設定

[プロキシ]画面の[アクセス制御設定]では、アクセス許可/禁止やキャッシュ許可/禁止、プロキシの使用許可/禁止というアクセスの制御が行えます。この設定は、最初に条件を持つリストを登録し、それぞれのリストに対しての 動作条件(アクセス制御、非キャッシュ設定、プロキシ転送)を設定していくという流れになります。デフォルトは、リスト設定に「リスト名:all ,設定種別:src ,条件式:0.0.0.0/0.0.0.0」、「リスト名:cgi ,設定種別:url_pathregex ,条件式:.cgi$ ¥?」、アクセス制御設定に「allow/deny:allow , リスト名:all」、非キャッシュ設定に「allow/deny:deny ,リスト名:cgi」です。

- **アクセス制御設定において、リストをまったく設定しない場合、または指定した条件のいずれにも該当しないアクセス要求は、「アクセスを許可する」として扱われます。**
- **アクセス制御設定、非キャッシュ設定、プロキシ転送設定合わせて最大100個まで設定することが可能です。**

リストを複数指定する際、<Shift>キーを押しながらクリックすることで範囲選択を、<Ctrl>キーを押しながらクリックすることで個別に選択することができます。

リスト設定

● リストの追加

リストを登録するには、アクセス制御の上画面に表示されている[リスト設定]画面から、[追加]をクリックします。

重要

- **設定種別でsrc、dst、myipを選択する場合、maskはマスクビット数で表わすことができる最上位bitから連続したbitが立つ値を指定してください。**
- **[設定]をクリックしないと、システムに反映されません。**

ヒント

- [追加]をクリックすることで、[リスト(追加)設定]画面を開くことができます。
- [リスト(追加)設定]画面で入力できるリスト名は、半角英数字16文字(先頭に数字は不可)以内です。
- 設定種別や条件式の詳細については、[ヘルプ]をクリックし、オンラインヘルプを参照してください。

● リストの編集

リストを編集するには、アクセス制御の上画面に表示されている[リスト設定]画面から編集したいリスト名の左横にある[編集]をクリックします。

重要

- **設定種別でsrc、dst、myipを選択する場合、maskはマスクビット数で表わすことができる最上位bitから連続したbitが立つ値を指定してください。**
- **[設定]をクリックしないと、システムに反映されません。**
- **設定項目の詳細については、[ヘルプ]をクリックし、オンラインヘルプを参照してください。**

ヒント

- [編集]をクリックすることで、[リスト(編集)設定]画面を開くことができます。
- [リスト(編集)設定]画面には、選択したリストの情報が表示されます。

● リストの削除

リストを削除するにはアクセス制御の上画面に表示されている[リスト設定]画面から削除したいリスト名の左横にある[削除]をクリックします。画面に削除するかどうかの確認を求めるダイアログボックスが表示されます。削除する場合は、[OK]をクリックしてください。

システムの管理

動作条件の設定

アクセス制御の下画面では、登録したリストに対して動作条件の設定を行います。3つの動作について設定することができます。

● **アクセス制御設定**

登録したリストに対して、アクセスの許可/禁止を設定します。

ー　アクセス制御の追加

アクセス制御リストを追加をするには、アクセス制御設定の[追加]をクリックします。

重要

- **[設定]をクリックしないと、システムに反映されません。**
- **設定項目の詳細については、[ヘルプ]をクリックし、オンラインヘルプを参照してください。**

ヒント

- [追加]をクリックすることで、[アクセス制御(追加)設定]画面を開くことができます。
- アクセス制御したいリストを選択し、アクセスの許可(allow)か禁止(deny)かを決定します。
- リストを複数指定した場合にはANDの処理が行われます。

ー　アクセス制御の編集

アクセス制御リストを編集するには、編集したいリスト名の左横にある[編集]をクリックします。

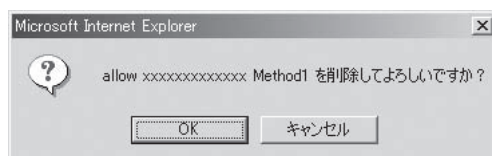
重要

- **[設定]をクリックしないと、システムに反映されません。**
- **設定項目の詳細については、[ヘルプ]をクリックし、オンラインヘルプを参照してください。**

ヒント

- [編集]をクリックすることで、[アクセス制御(編集)設定]画面を開くことができます。
- [アクセス制御(編集)設定]画面には、選択したリストの情報が表示されます。

— アクセス制御の削除

アクセス制御リストを削除するには、削除したいリスト名の左横にある[削除]をクリックします。画面に削除するかどうかの確認を求めるダイアログボックスが表示されます。削除する場合は、[OK]をクリックしてください。

— 順序の設定

アクセス制御の順序を設定することができます。[順序]をクリックすると、順序設定画面が表示されます。優先度を変更したいリストを選択し、[UP]、[DOWN]をクリックすることで設定することができます。

重要

- **順序は一番上が優先度が高く、下に行くにつれて優先度が低くなります。**
- **[実行]をクリックしないと、システムに反映されません。**

● **非キャッシュ設定**

登録したリストに対して、キャッシュしてもよい/いけないを設定します。

非キャッシュ設定	allow/deny	リスト名
追加 順序	allow/deny	リスト名
編集 削除	allow	Method1

— 非キャッシュ設定の追加

非キャッシュ設定リストを追加をするには、非キャッシュ設定の[追加]をクリックします。

重要

- **[設定]をクリックしないと、システムに反映されません。**
- **設定項目の詳細については、[ヘルプ]をクリックし、オンラインヘルプを参照してください。**

ヒント

- [追加]をクリックすることで、[非キャッシュ（追加）設定]画面を開くことができます。
- キャッシュ制御したいリストを選択し、キャッシュの許可（allow）か禁止（deny）かを決定します。
- リストを複数指定した場合にはANDの処理が行われます。

— 非キャッシュ設定の編集

非キャッシュ設定リストを編集するには、編集したいリスト名の左横にある[編集]をクリックします。

重要

- **[設定]をクリックしないと、システムに反映されません。**
- **設定項目の詳細については、[ヘルプ]をクリックし、オンラインヘルプを参照してください。**

ヒント

- [編集]をクリックすることで、[非キャッシュ(編集)設定]画面を開くことができます。
- [非キャッシュ(編集)設定]画面には、選択したリストの情報が表示されます。

— 非キャッシュ設定の削除

非キャッシュ設定リストを削除するには、削除したいリスト名の左横にある[削除]をクリックします。画面に削除するかどうかの確認を求めるダイアログボックスが表示されます。削除する場合は、[OK]をクリックしてください。

— 順序の設定

非キャッシュ設定の順序を設定することができます。[順序]をクリックすると、順序設定画面が表示されます。優先度を変更したいリストを選択し、[UP]、[DOWN]をクリックすることで設定することができます。

重要

- **順序は一番上が優先度が高く、下に行くにつれて優先度が低くなります。**
- **[実行]をクリックしないと、システムに反映されません。**

● **プロキシ転送設定**

登録したリストに対して、隣接プロキシを使用する/しないを設定します。

プロキシ転送設定				
追加	順序	転送種別	allow/deny	リスト名
編集	削除	Always_direct	allow	xxxxxxxxxxxxx

ー　プロキシ転送設定の追加

プロキシ転送設定リストを追加するには、プロキシ転送設定の［追加］をクリックします。

重要

［設定］をクリックしないと、システムに反映されません。

ヒント

- ［追加］をクリックすることで［プロキシ転送（追加）設定］画面を開くことができます。
- プロキシ転送を必ず行う（Always_direct）か、行わない（Never_direct）を［転送種別］から選択します。
- それぞれの設定に対して、許可する（allow）、許可しない（deny）を設定します。
- リストを複数指定した場合にはANDの処理が行われます。
- 設定項目の詳細については、［ヘルプ］をクリックし、オンラインヘルプを参照してください。

ー　プロキシ転送設定の編集

プロキシ転送設定リストを追加をするには、プロキシ転送設定の［編集］をクリックします。

重要

［設定］をクリックしないと、システムに反映されません。

ヒント

- ［編集］をクリックすることで、［プロキシ転送（編集）設定］画面を開くことができます。
- ［プロキシ転送設定（編集）設定］画面には、選択したリストの情報が表示されます。
- 設定項目の詳細については、［ヘルプ］をクリックし、オンラインヘルプを参照してください。

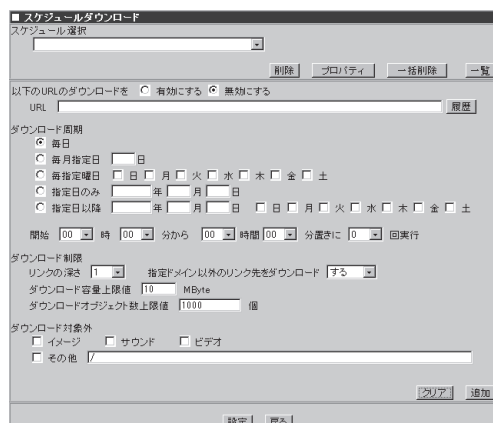
－　プロキシ転送設定の削除

プロキシ転送設定リストを削除するには、削除したいリスト名の左横にある［削除］をクリックします。画面に削除するかどうかの確認を求めるダイアログボックスが表示されます。削除する場合は、［ＯＫ］をクリックしてください。

－　順序の設定

プロキシ転送設定の順序を設定することができます。［順序］をクリックすると、順序設定画面が表示されます。優先度を変更したいリストを選択し、［UP］、［DOWN］をクリックすることで設定することができます。

重要

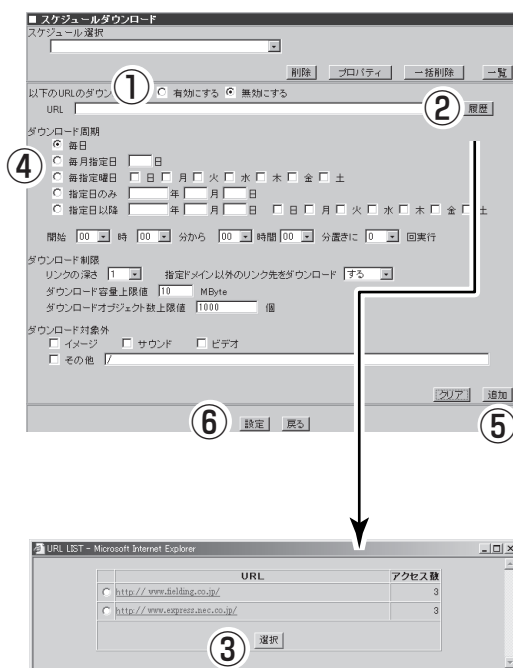
- **順序は一番上が優先度が高く、下に行くにつれて優先度が低くなります。**
- **［実行］をクリックしないと、システムに反映されません。**
- **プロキシ転送設定で「Never_direct（転送しない）」を設定すると、直接Webサーバへ接続しようとします。親プロキシが複数ある場合などはご注意ください。**

スケジュールダウンロード

スケジュールダウンロードとは、指定したページをあらかじめ指定時刻にダウンロードし、キャッシュ可能であればキャッシュする機能です。
対象となるURL、ダウンロード周期などスケジュールダウンロードの設定ができます。

重要

- **コンテンツの性質とサイズによってはキャッシュされないこともあります。**
- **対象コンテンツ(URL)がキャッシュ可能である場合は、対象コンテンツへのアクセスがアクセスログのキャッシュステータス結果でHITになっています。**

スケジュールの新規追加

スケジュールを追加するには、対象となるURL、ダウンロード周期などを設定し[追加]をクリックします。スケジュールは最大100件まで追加できます。下に示す図と手順の流れの関係は次のとおりです。

1. 「有効にする」を選択する。
2. ダウンロードするURLを入力する。

   例） http://nec8.com/
3. [履歴]をクリックする。

   [URL LIST]画面が表示されます。
4. [追加]をクリックしてダウンロードしたいURLを追加する。
5. [設定]をクリックする。

履歴機能が有効になるのは、[システム]画面の[プロキシアクセス統計]でプロキシアクセス統計を「有効にする」を設定した時だけです。

設定項目の詳細については、[ヘルプ]をクリックし、オンラインヘルプを参照してください。

スケジュールの変更

スケジュールを変更するには、[スケジュール選択]欄からスケジュールを選択し、変更したい項目を編集します。

[設定]をクリックしないと、システムに反映されません。

ヒント

- 引き続き別のスケジュールを編集するときは、そのまま一覧から選択してください。編集内容はウィンドウ内で一時保存されます。
- 設定項目の詳細については、[ヘルプ]をクリックし、オンラインヘルプを参照してください。

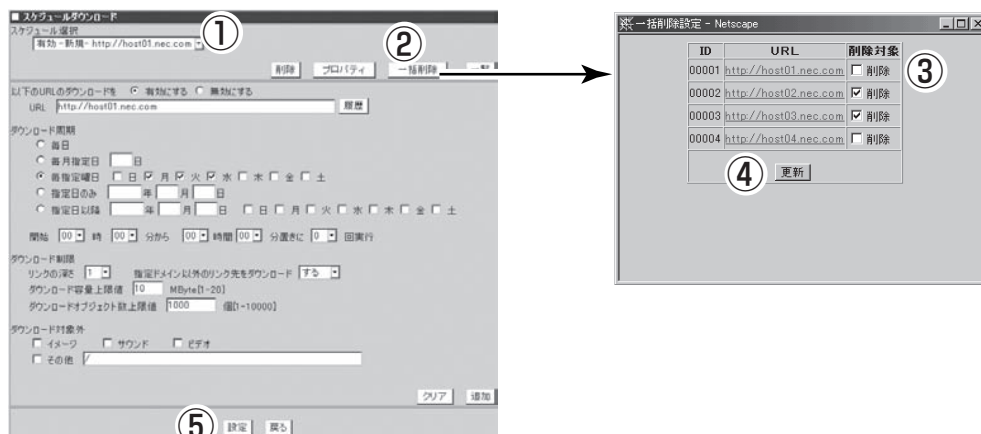
スケジュールの削除

スケジュールを削除するには、[スケジュール選択]欄からスケジュールを選択し、[削除]をクリックします。

[設定]をクリックしないと、システムに反映されません。

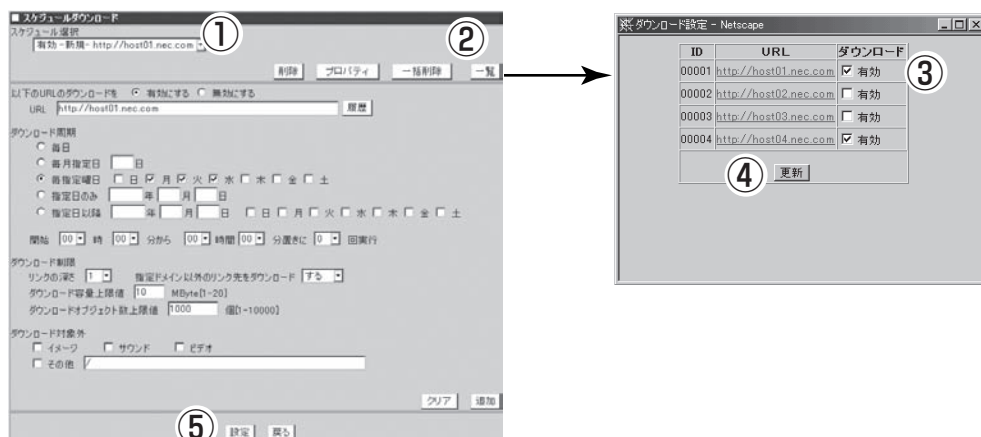
スケジュールの一括削除

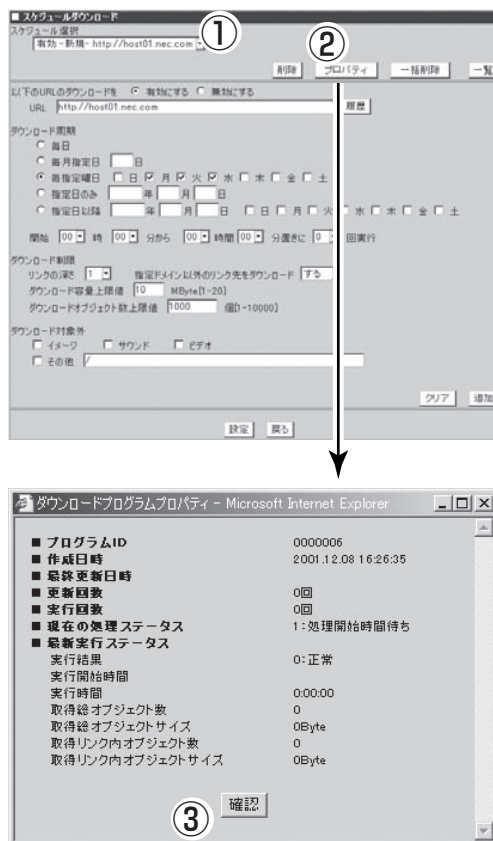
［一括削除］をクリックすることで［一括削除設定］画面を開くことができます。［一括削除設定］画面で、削除したいスケジュールの［削除対象］をチェックし［更新］をクリックすると、［スケジュール選択］欄から削除されます。

重要　**［設定］をクリックしないと、システムに反映されません。**

スケジュールの一括設定

［一覧］をクリックすることで［ダウンロード設定］画面を開くことができます。［ダウンロード設定］画面で、ダウンロードを実行したいスケジュールの［ダウンロード］をチェックし［更新］をクリックすると、［スケジュール選択］欄に反映されます。

重要　**［設定］をクリックしないと、システムに反映されません。**

ダウンロードを実行する時は［ダウンロード］にチェックを付け、実行しない時はチェックを外してください。

スケジュールの確認

[プロパティ]をクリックすると、選択したスケジュールの設定履歴や最新のダウンロード結果などを表示します。

認証設定

[プロキシ]画面の[認証設定]で、システムを使用するユーザを認証するための設定ができます 。

特定のアクセスに対して認証機能をスキップさせたい場合は、「特殊アクセス制御設定」で設定を行うことができます。

バイパス設定

[プロキシ]画面の[バイパス設定]では、システムを透過型プロキシとして動作させる際の、静的バイパス･動的バイパスの設定を行います。

特殊アクセス制御設定

認証サービスをスキップさせる「認証スキップ設定」、URLフィルタリングソフトをスキップさせる「URLフィルタスキップ設定」、Keep-Alive接続の方法について細かく指定する「Keep-Alive設定」などの各種例外設定を行います。
設定対象となるリストは、「アクセス制御設定」と共有します。

SSLアクセラレータ設定(リバースプロキシ用)

リバースプロキシサーバでSSLアクセラレータ機能を使用する設定を行います。
本機能は、オプション機能です。使用するためには、ライセンスをインストールしてください。

フィルター選択

[プロキシ]画面の[フィルター選択]画面で、使用するフィルタリングソフトを選択することができます。フィルタリングソフトはInterSafe、InterScan WebManagerを使用することができます。
ご利用の際は、InterSafeはライセンスの追加のみ、InterScan WebManagerはオプションソフトのインストールとライセンスの追加が必要です。
フィルタリングソフトの対応バージョンは、随時サポートサイトなどでご確認ください。
InterSafe使用時は、アクセスログへフィルタリングカテゴリ名およびフィルタリング結果を表示させることができます。

InterScan WebManager・InterSafeのログローテート設定

InterScan WebManagerやInterSafeの各管理コンソールでログローテートの設定をする場合、その合計ファイルサイズに注意してください。本システムでは、約6GBのディスク容量を設けています。万一の障害発生時のメモリダンプ採取用の空き領域(搭載メモリ分)+InterScan WebManager、InterSafeのインストール用領域(約100MB)+InterScan WebManager、InterSafeのログファイルの合計が6GBを超えないよう、余裕を持たせた設定にしてください。
また、RAID構成の場合はManagementConsoleで設定できる各種ログファイルのサイズも含めて合計6GB以内となるように設定してください。

重要

- **InterScan WebManagerを一度インストールするとアンインストールすることはできません。**
- **InterSafeを使用していて、他ソフトを使用したくなった場合にはいったん「フィルタリングソフトを使用しない」を設定してから他ソフトを使用してください。**
- **InterSafeまたはInterScan WebManagerを使用する場合は、Management Consoleに加えて、各製品の管理コンソールでの設定が必要です。**
- **InterSafeの管理画面を起動させるには、「サービス」画面の「InterSafe」を起動させる必要があります。なお、InterSafeの利用をやめる場合は、「サービス」画面でInterSafeを停止させてください。**

InterScan WebManager設定

[プロキシ]画面の[フィルター選択]画面の[InterScan WebManager動作設定]で、InterScan WebManagerの設定を行います。この設定はInterScan WebManagerを本システムで使用するとき必ず必要です。IPアドレスとポート番号の指定はInterScan WebManagerで設定する内容に従って設定してください。なお、この画面でIPアドレスとポート番号を変更してもInterScan WebManagerには反映されません。

InterScan WebManagerインストール手順

InterScan WebManagerのインストール手順を示します。

1. [システム]画面の[保守用パスワード]でmainteユーザのパスワードを設定する。
2. [サービス]画面で「リモートログイン(telnetd)」を起動する。
3. [サービス]画面の「リモートログイン(telnetd)」をクリックして[リモートログイン(telnetd)]画面へ遷移し、本システムにリモートログインできるようにTelnetを許可するホストを設定する。
4. Telnetでmainteユーザで本システムにリモートログインし、「su -」とコマンドラインに打ち込む。
5. パスワードを求められるので、Management Consoleにログインするためのパスワード(adminのパスワード)を指定する。

   管理者ユーザになります。
6. InterScan WebManagerのマニュアルに基づきインストールをする。

   InterScan WebManagerインストール中にインストールディレクトリを聞かれますが、「/usr/local」を指定します。
7. InterScan WebManagerのインストール後、[プロキシ]画面の[フィルター選択]で「InterScan WebManagerを使用する」を指定し、「設定」をクリックして現れる[InterScan WebManager動作設定]画面にてInterScanのIPアドレスやポート番号を指定する。

   IPアドレスやポート番号を指定し、[設定]をクリックします。
8. [システム]画面にて[システムの再起動]を実行する。

InterSafe設定

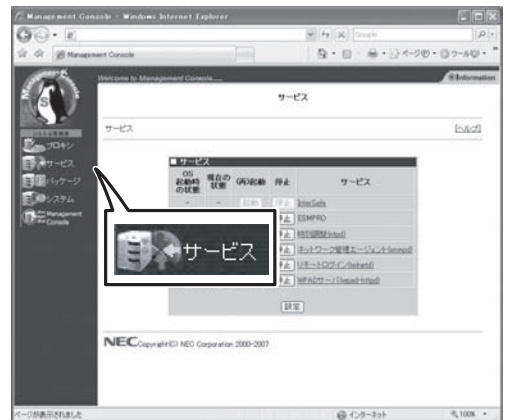
[プロキシ]画面の[フィルター選択]画面の[InterSafe設定]で、InterSafeの設定を行います。この設定はInterSafeを本システムで使用するとき必要ですので、必ず行ってください。IPアドレスとポート番号などの指定は、「サービス」画面からInterSafe管理コンソールを起動し、表示する内容に従って設定してください。なお、本画面でIPアドレスとポート番号を変更してもInterSafe管理コンソールには反映されません。

InterSafe管理コンソールでInterSafeのIPアドレスやポート番号を変更した場合には必ずこの画面の設定も変更してください。

- InterSafe設定で設定を行った後、[プロキシ]画面に[InterSafe設定]の項目が表示されるようになります。
- InterSafeのマニュアルは、インストールCD-ROM内のmanual.htmlから閲覧できます。

サービス

管理者は、Management Consoleから以下のサービスの設定を簡単に行うことができます。

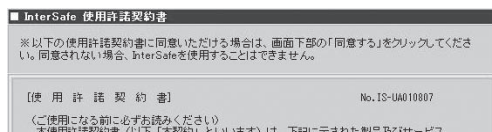
- InterSafe
- 時刻調整（ntpd）
- ネットワーク管理エージェント（snmpd）
- リモートログイン（telnetd）
- WPADサーバ（wpad-httpd）

サービス画面では各機能の停止･起動を指示可能で、現在の稼動状況を表示します。さらにここから、各機能ごとの詳細な設定を行う画面に移ります。

- OS起動時の状態:　システムが起動した際に、このサービスを自動的に有効にするかどうかを指定します。
- 現在の状態:　現在、このサービスが動作しているかどうかを表示します。
- （再）起動:　このサービスが停止している場合に起動します。動作中の場合には、停止させてから再起動します。
- 停止:　このサービスが動作中であれば、停止します。

InterSafe

ICAP(Internet Content Adaptation Protocol)によるURLフィルタリングを行えます(InterSafeをICAPサーバとして使用)。

フィルタリングソフトウェアでのプロキシ動作が不要となるため、処理性能が向上します。

初めて利用する際は、右側の「InterSafe」のリンクをクリックし、使用承諾契約書の内容をよく読んで「同意する」ボタンをクリックしてください。

- 本画面では、InterSafe管理用コンソールの起動/停止を設定することができます。InterSafeを利用するには、「プロキシ」→「フィルター設定」画面でもInterSafeの設定が行われている必要があります。
- InterSafeの使用をやめる場合は、「プロキシ」→「フィルター設定」画面で変更を行い、「サービス」→「InterSafe」画面でInterSafeを停止してください。

時刻調整(ntpd)

NTP(Network Time Protocol)は、ネットワークで接続されたコンピュータ同士が連絡を取り合い、時計のずれを自動的に調整する仕組みです。本システムはこの仕組みを利用して、以下の機能を提供しています。

- インターネットの標準時刻サーバに、本システムの時計を合わせる。
- 他のPCが時計を本システムに合わせるのに必要な情報を提供する。

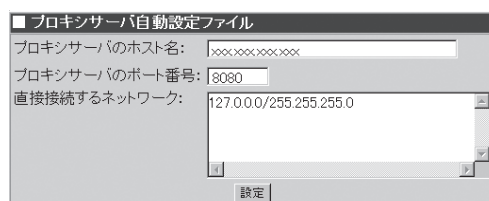
ネットワーク管理エージェント(snmpd)

SNMP(Simple Network Management Protocol)は、ネットワークに接続された機器の稼動状況を、ネットワークを通じて取得するための仕組みです。本システムは、ネットワークに接続された機器(エージェント)の側として、必要な情報をネットワークに発信する機能を提供しています。

リモートログイン(telnetd)

他のコンピュータ(ホスト)から本システムに接続することを可能にする機能です。Management Consoleでは対応できない特別な操作を行いたい場合にだけこの機能を有効にします。通常の運用時に有効にする必要はありません。有効にしている間はセキュリティのレベルが低下しますので、通常は無効にしておくことをお勧めします。
「Telnetログインを許可するホスト」画面にて、ログイン可能なホストを各種形式で指定します。カンマで区切って複数のホストを指定可能です。IPアドレスやホスト名以外にも各種指定形式をサポートしています。指定形式の詳細については画面右上のオンラインヘルプを参照してください。

WPADサーバ(wpad-httpd)

本システムをフォワードプロキシとして利用している際に、ブラウザ側でのプロキシ設定を自動化するための機能です。Internet Explorer 5以降で対応しています。本機能を利用するためには、ブラウザの参照しているDNSサーバおよびDHCPサーバを適切に設定する必要があります。
[プロキシサーバ自動設定ファイル]画面で本システムに接続する際に使用するホスト名とポート番号を設定します。本システムを通さないで接続すべきマシンがあれば、ネットワークアドレス単位で指定することが可能です。

重要 **WPADサーバは本システムのサーバ種別を「Forward(透過型L4スイッチ)」、「Forward(透過型WCCP)」または「Reverse」に設定した時にはご利用できません。**

パッケージ

本システムにインストールされているアプリケーションなどのソフトウェアパッケージのアップデートやインストール、インストールされているパッケージの一覧を確認する画面です。

オンラインアップデート

オンラインアップデートを利用すると、Management Consoleから簡単にアップデートモジュールをインストールすることができます。
アップデートモジュールとは、本システムに追加インストール（アップデート）可能なソフトウェアで、弊社で基本的な動作確認を行って公開しているものです。 内容は、既存ソフトウェアの出荷後に発見された不具合修正や機能追加などが主ですが、新規ソフトウェアが存在することもあります。オンラインアップデートでは、現在公開されている本システム向けのアップデートモジュールの一覧を参照し、安全にモジュールをインストールすることができます。

重要

- **アップデートモジュールを適用後も適用状態が「未」と表示される場合は、モジュールの適用に失敗したか、システムの再起動を行っていない可能性があります。**
- **オンラインアップデート時は、本サーバがクライアントとなり、アップデートWeb用サーバへ接続します。「取得用proxyアドレス」に本サーバを設定している場合、事前に以下の画面で自身からのアクセスを受け付ける設定にしておいてください。**

  ・[プロキシ]→[アクセス制御設定]画面

  ・[プロキシ]→[セキュリティ設定]画面

手動インストール

ローカルディレクトリのファイル名、またはURL、PROXY、PORTを指定してRPMパッケージをインストールすることができます。

パッケージの一覧

現在本システムにインストールされているRPMパッケージの一覧を確認することができます。また、アンインストール作業を行うこともできます。

システム

Management Console画面左の[システム]アイコンをクリックすると「システム」画面が表示されます。

システムの停止

[システムの停止]をクリックすると「システムを停止します。

システムの再起動

[システムの再起動」をクリックすると「システムを再起動します。

CPU/メモリ使用状況

メモリの使用状況とCPUの使用状況をグラフと数値で表示します。約10秒ごとに最新の情報に表示が更新されます。
また、CPU使用率と負荷について、調節を行うことができます（上級者向け）。設定を変更する場合は、環境や使用状況にあわせて適当な値をチューニングしてください。

ディスク使用状況

ディスクの使用状況を各ファイルシステムごとに数値とグラフで表示します。空き容量、使用率に注意してください。空き容量が足りなくなるとシステムが正常に動作しなくなる可能性があります。

プロセス実行状況

現在実行中のプロセスの一覧を表示します。プロセス実行状況の表の最上行の項目名をクリックすると、各項目で表示をソートすることができます。表示項目の詳細については、[ヘルプ]をクリックし、オンラインヘルプを参照してください。

名前解決診断

ネットワーク設定で登録されているDNSサーバの動作を確認することができます。
「ホスト:」に適当なホスト名を入力して[診断]をクリックすると診断結果が表示されます。ホスト名に対して正しく「Name:」と「Address:」が表示されればDNSサーバは正常に機能しています。

ネットワーク利用状況

ネットワーク利用状況を表示します。
[約5秒毎に画面をリフレッシュする]チェックボックスをチェックすると自動的に表示が最新状況に更新されます。

ネットワーク接続状況

各ポートごとの接続状況を表示します。
[約5秒毎に画面をリフレッシュする]チェックボックスをチェックすると自動的に表示が最新状況に更新されます。

プロキシアクセス統計

アクセスの統計情報を表示します。[プロキシアクセス統計表示]画面の「Summary by Month」の表の[Month]の項目のリンクをクリックするとその月の詳細な統計情報を表示します。
プロキシアクセス動作設定はプロキシアクセス統計を有効にして動作させるかどうか設定します。
動作させる際には優先度を設定してください。優先度は1から20まで設定可能であり、値が大きいほど優先度が低くなります。優先度を低くすることによりプロキシアクセス統計の動作によるCPUの負荷を減らすことができます。
Webalizer表示設定では、sitesはサイト別上位を、sites By KBytesはサイト別キロバイト上位を、URL'sはURL上位を、URL's By KBytesはサイト別キロバイト上位をEntry Pagesは入り口上位を、Exit Pagesは出口別上位をいくつまで表示するか設定することができます。

重要

- **プロキシアクセス統計を無効にするを選択するとそれまで作成されていた統計情報は削除されます。**
- **プロキシアクセス統計を動作させると性能低下がおこる可能性があります。**
- **優先度は慎重に決定してください。低い優先度を設定するとシステムの負荷状況によっては正常に統計情報が作成されない可能性があります。**
- **プロキシアクセス統計情報を動作させると、キャッシュサーバのアクセスログのログ出力形式はSquidに、ローテート世代数は「1」に固定され、ローテートサイズはいったん100MBに設定されます。**
- **プロキシアクセス統計を動作させている時、ローテートサイズの扱いには注意してください。システムの性能およびプロキシアクセス統計の動作に影響を与えます。**

- ［初期値］をクリックすると、それぞれのテキストボックスに初期値が入ります。
- 各テキストボックスは0～99まで入力することができます。
- 統計情報はシステムのアクセスログがローテートされたときに作成されます。
- システムのアクセスログのローテートの設定は［システム］画面の［ログ設定］画面の［キャッシュサーバアクセスログ］の［設定］をクリックすることで表示される［キャッシュサーバアクセスログ設定］画面にて行えます。

経路情報

「相手ホスト:」にホスト名を入力して［表示］をクリックすると、そのホストまでの経路情報を表示します。

システム情報

装置に割り当てたホスト名、およびOSに関する情報を表示します。

AFT/ALB設定

AFT（Adapter Fault Tolerance）/ALB（Adaptive Load Balancing）モードの設定を行います。

ネットワーク

ネットワークの基本的な設定やネットワークインタフェース、ルーティングの設定を行います。

AFT/ALBの設定を行っているときは、eth1に対する設定はできません。

アクセスログ取得

キャッシュサーバアクセスログをSambaまたはFTPで指定したホストを利用して転送します。

本システムのアクセスログのローテートの設定は［システム］画面の［ログ管理］画面の［キャッシュサーバアクセスログ］の［設定］をクリックすることで表示される［キャッシュサーバアクセスログ設定］画面にて行えます。

バックアップ/リストア

ファイルのバックアップおよびリストアの設定を行います。詳細はこの後に説明する「バックアップ/リストア」を参照してください。

管理者パスワード

管理者(admin)のパスワードを変更します。各パスワードは6文字以上8文字以下の半角英数文字(半角記号を含む)を指定してください。省略すると、パスワードは変更されません。空のパスワードを指定することはできません。
また、管理者宛のメールを転送する先を設定できます。管理者宛メールの転送先は正しく送信できるアドレスを指定してください。

ログ管理

ログの表示、ログのローテートの設定を行います。
ログの表示は表示したいログの[表示]をクリックするとローテートされたログの一覧が表示され、その中から表示したいログを選択して表示します。
ログのローテートの設定は、ローテートを行うタイミングを周期またはファイルサイズで指定し、何世代までログを残すかを設定します。

- **ログのローテートは毎日0:00とシステム起動時にチェックし、条件があっているものをローテートします。**
- **ログのローテートのタイミングでシステムの停止および再起動を行う場合にはご注意ください。**
- **キャッシュサーバアクセスログの設定は他のログと異なります。詳細は次に説明する「キャッシュサーバアクセスログ」を参照してください。**

ヒント

ログを表示したとき、ログのダウンロードを行うことも可能です。

キャッシュサーバアクセスログ

キャッシュサーバアクセスログの[設定]をクリックすると、[キャッシュサーバアクセスログ設定]画面が表示されます。この画面は、キャッシュサーバアクセスログの出力形式、ローテート(条件、サイズ、時間、時刻)、何世代までログを残すかなどを設定することができます。出力形式が拡張形式であったとき、拡張形式でチェックボックスにチェックを入れた項目がログ出力されます。

アクセスログ取得、プロキシアクセス統計情報を動作させている時はローテートサイズの扱いに注意してください。システムの性能に影響を与えます。

バックアップ/リストア

システムの故障、設定の誤った変更など思わぬトラブルからスムーズに復旧するために、定期的にシステムのファイルのバックアップをとっておくことを強く推奨します。
バックアップしておいたファイルを「リストア」することによってバックアップを作成した時点の状態へシステムを復元することができるようになります。
本装置では、システム内のファイルを以下の5つのグループに分類して、その各グループごとにファイルのバックアップのとり方を制御することができます。
それぞれのグループのバックアップ対象ディレクトリおよび作成されるファイルの名称は以下の通りです 。

- **システムの設定ファイル**

  対象ディレクトリ　: /etc 配下
  　圧縮(ローカル) : backup_conf_*.tgz
  　圧縮(Samba)　 : backup_smb_conf_*.tgz

- **プロキシサーバの設定ファイル**

  対象ディレクトリ　: /etc/crontab
  　　　　　　　　　　/opt/nec/ catfish、roma、smartfilter 配下
  　圧縮(ローカル) : backup_proxy_*.tgz
  　圧縮(Samba)　 : backup_smb_proxy_*.tgz

- **各種ログファイル**

  対象ディレクトリ　: /var/lib/logrotate.status　var 配下
  　　　　　　　　　　/var/log 配下
  　圧縮(ローカル) : backup_log_*.tgz
  　圧縮(Samba)　 : backup_smb_log_*.tgz

- **プロキシアクセス統計情報**

  対象ディレクトリ　: /home/webalizer/ 配下
  　圧縮(ローカル) : backup_alizer_*.tgz
  　圧縮(Samba)　 : backup_smb_alizer_*.tgz

- **ディレクトリ指定**

  対象ディレクトリ　:　任意のディレクトリ
  　　　　　　　　　　*　例えば、フィルタリングソフト(InterSafe)関連のファイルを指定する場合、/usr/local/intersafe/ を指定します。
  　圧縮(ローカル) : backup_dirinfo_*.tgz
  　圧縮(Samba)　 : backup_smb_dirinfo_*.tgz

初期状態では、いずれのグループも「バックアップしない」設定になっています。お客様の環境にあわせて各グループのファイルのバックアップを設定してください。
本装置では各グループに対して「ローカルディスク」と「Samba」の2種類のバックアップ方法を指定することができます。
各方法には、それぞれ以下のような特徴があります。

- **ローカルディスク**

  内蔵ハードディスクの別の場所にバックアップをとります。

- **Samba**

  ＬＡＮに接続されているWindowsマシンのディスクにバックアップをとります。

バックアップ方式にローカルディスクを指定する場合、ディスクフルを起こさないよう注意してください。
ディスクフルになると、プロキシサービスが停止します。
使用可能なディスク容量は、システムのディスク使用状況画面でマウントポイント「/」で表示されている容量です。
標準構成の場合、以下の合計が使用可能なディスク容量を超えないよう、余裕を持たせた設定にしてください。

・ 万一の傷害発生時のメモリダンプ採取用の空き領域（搭載メモリ分）
・ InterScan WebManager、InterSafeのインストール用領域（約100MB）
・ InterScan WebManager、InterSafeのログファイル
・ バックアップファイル
・ システムのログ管理画面で設定できる各種ログファイル

重要

- **システムの設定ファイル、およびプロキシサーバの設定ファイルは必ずバックアップを設定してください。**
- **ローカルディスクへのバックアップは、他の方法に比べてリストアできない可能性が高くなります。なるべくＳａｍｂａを使用して、別マシンへバックアップをとるようにしてください。**
- **Ｓａｍｂａでのバックアップは、内蔵ハードディスクがクラッシュしても復元を行うことができますが、あらかじめ、Ｗｉｎｄｏｗｓマシンに共有の設定をしておく必要がありますので注意してください。**
- **キャッシュサーバアクセスログおよびキャッシュログは、「各種ログファイル」のバックアップでの対象外となりますので、注意してください。**

「Samba」によるバックアップ設定の例

ここでは「Samba」を使用したバックアップの方法について説明します。
例として「workgroup」内に所属するマシン名「winpc」というWindowsマシンの「C:ドライブ」にバックアップのためのフォルダ「cachebackup」を作成して「システムの設定ファイル」グループのファイルのバックアップを行う場合の操作手順を説明します。
バックアップファイルを置くマシン(winpc)でのバックアップ作業のためのユーザーを「winpc」上にあらかじめ用意してください。

バックアップファイルの中にはシステムのセキュリティに関する情報などが含まれるため、バックアップのためのフォルダ(cachebackup)の読み取り、変更の権限などのセキュリティの設定には十分注意してください。(Windows Me/98/95ではセキュリティの設定ができません。そのためお客様の情報が第三者に盗まれる可能性があります。)

バックアップ作業のためのユーザーは既存のユーザーでもかまいませんが、以下の説明では「cacheadmin」というユーザーをあらかじめ用意したという前提で説明します。

次の順序で設定します。以降、順に設定例を説明していきます。

1. Windowsマシンの共有フォルダの作成
2. システムのバックアップファイルグループの設定
3. バックアップの実行

バックアップ用に作成した共有フォルダの設定を不用意に変更するとシステムのバックアップおよび復元の機能が正常に動作しなくなるので注意してください。

Windowsマシンの共有フォルダの作成

まず、バックアップファイルを置いておくための共有フォルダをWindowsマシンに作成します。ここでは、例としてWindows 2000、Windows XPの2種のOSでの作成方法を説明します。

操作例:winpcのOSがWindows XPの場合

1. マシン「winpc」の[マイコンピュータ]画面を開く。

2. 開いた[マイコンピュータ]ウインドウの[C:ドライブ]のアイコンをダブルクリックする。

3. [ファイル]メニューの[新規作成]→[フォルダ]をクリックする。

4. ［新しいフォルダ］の名前に［cachebackup］とキーボードから入力し<Enter>キーを押す。

5. 上記の手順で作成した［cachebackup］フォルダをクリックして選択する。

6. ［ファイル］メニューの［共有とセキュリティ］をクリックする。

［cachebackupのプロパティ］ウインドウの［共有］シートが表示されます。

7. ［ネットワーク上での共有とセキュリティ］メニューで、［ネットワーク上でこのフォルダを共有する］のチェックボックスと［ネットワークユーザによるファイルの変更を許可する］にチェックをつける。

8. ［OK］をクリックして［cachebackupのプロパティ］のウインドウを閉じる。

9. ［cachebackup］フォルダのアイコンが変わったことを確認する。

以上でWindowsXP上の共有フォルダの設定は完了です。

操作例：winpcのOSがWindows 2000の場合

1. マシン「winpc」のデスクトップ上にある［マイコンピュータ］をダブルクリックする。

2. 開いた［マイコンピュータ］ウィンドウの［C：ドライブ］のアイコンをダブルクリックする。

3. ［ファイル］メニューの［新規作成］→［フォルダ］をクリックする。

4. ［新しいフォルダ］の名前に［cachebackup］とキーボードから入力し<Enter>キーを押す。

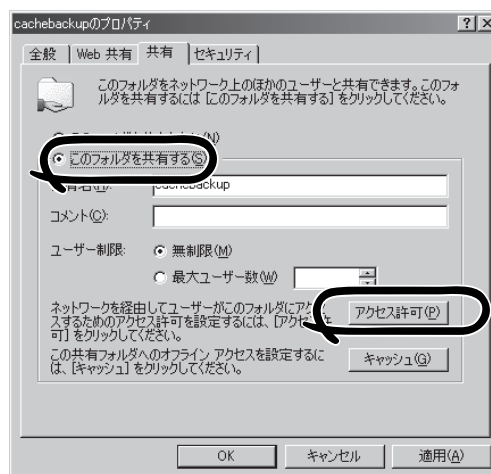
5. 上記の手順で作成した［cachebackup］フォルダをクリックして選択する。

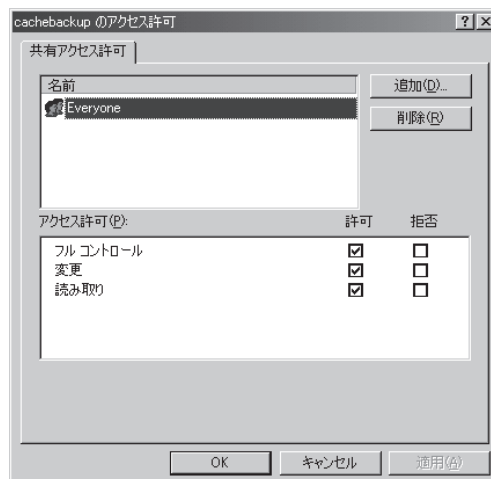
6. [ファイル]メニューの[共有]をクリックする。

   [cachebackupのプロパティ]ウィンドウの[共有]シートが表示されます。

7. [このフォルダを共有する]をクリックする。

8. [アクセス許可]をクリックする。

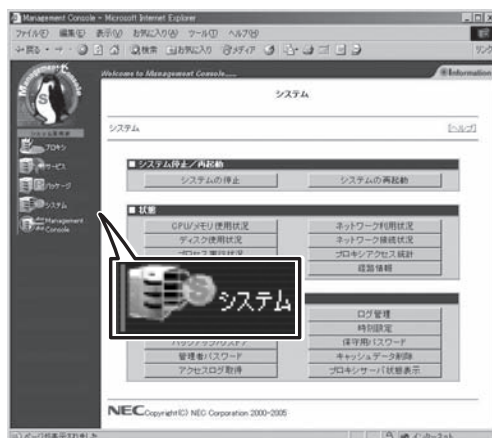
9. [共有アクセス許可]を設定する。

   ここでは以下のように設定します。

   1. [名前]一覧から[Everyone]を削除する。
   2. [追加]をクリックして[ユーザー、コンピューター、またはグループの選択]ウィンドウでユーザー[cacheadmin]を追加して[OK]をクリックする。
   3. [共有アクセス許可]の[アクセス許可]一覧の[フルコントロール]の許可のチェックボックスにチェックをつける。

10. [OK]をクリックして[cachebackupのアクセス許可]のウィンドウを閉じる。

11. [OK]をクリックして[cachebackupのプロパティ]のウィンドウを閉じる。

12. [cachebackup]フォルダのアイコンが変わったことを確認する。

以上でWindows 2000上の共有フォルダの設定は完了です。

システムのバックアップファイルグループの設定

ここでは例として[システムの設定ファイル]グループのバックアップの設定手順を説明します(他のグループも操作方法は同じです)。

1. Management Console画面左の[システム]アイコンをクリックする。

   [システム]画面が表示されます。

2. [システム]画面の[その他]一覧の[バックアップ/リストア]をクリックする。

   [バックアップ/リストア一覧]画面が表示されます。

3. 一覧の[システムの設定ファイル]の左側の[編集]をクリックする。

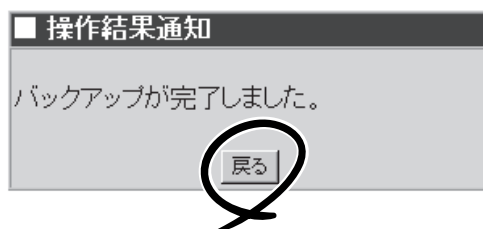
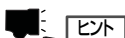
   バックアップ設定の[編集]画面が表示されます。

■ バックアップ/リストア一覧

操作	説明	世代数	タイミング
バックアップ 編集 リストア	システムの設定ファイル	5	バックアップしない
バックアップ 編集 リストア	プロキシサーバの設定ファイル	5	バックアップしない
バックアップ 編集 リストア	各種ログファイル	5	バックアップしない
バックアップ 編集 リストア	プロキシアクセス統計情報	5	バックアップしない

4. [編集]画面のバックアップ方式の[Samba]をクリックして選択する。

5. 「Windowsマシンの共有フォルダの作成」で行った設定に従って以下の項目を入力する。

   - ワークグループ(NTドメイン名): workgroup
   - [Windowsマシン名]: winpc
   - [共有名]: cachebackup
   - [ユーザ名]: cacheadmin
   - [パスワード]: ユーザcacheadminのパスワード

6. 正しく設定されていることを確認するため[即実行]をクリックしてバックアップを実行する。

   正しく実行された場合は右の操作結果通知が表示されます。

正しく操作結果通知が表示されない場合はWindowsマシンの共有の設定とバックアップ方式の設定が正しいかどうか確認してください。

ヒント

この[即実行]を使うことで、任意のタイミングで手動でバックアップを行うことができます。

7. [戻る]をクリックする。

定期的に自動的にバックアップを行うには次の設定を続けて行ってください。

8. [編集]画面で[世代]、[スケジュール]、[時刻]を指定する。

   右図の例では[毎週月曜日の朝9:00にバックアップをとる。バックアップファイルは3世代分残す]設定を行う場合を示しています。

世代

バックアップファイルをいくつ残すかを指定します。バックアップファイルを保管するディスクの容量と、必要性に応じて指定してください。世代を1にすると、バックアップを実行するたびに前回のバックアップ内容を上書きすることになります。

スケジュール

バックアップを実行する日を指定します。[毎日]、[毎週]、[毎月]、および[バックアップしない]から選択します。

[毎週]を指定する場合は右側の曜日も選択してください。

[毎月]を指定する場合は右側のテキストボックスに日付を入力してください

いずれの場合も指定した日付に本体の電源とバックアップ先のマシンの電源が入っていない場合はバックアップできないので注意してください。

時刻

[スケジュール]で指定した日付の何時何分にバックアップを行うかを指定します。指定した時刻に本体の電源とバックアップ先のマシンの電源がONになっていない場合はバックアップできないので注意してください。

9. ［編集］画面下の［設定］をクリックする。

以上で、定期的に自動的にバックアップを行う設定は完了です。

バックアップの実行

バックアップの処理は「システムのバックアップファイルグループの設定」で指定した日時に本体の電源とバックアップ先のマシンの電源が入っていない場合は、バックアップされませんので注意してください。

リストア

バックアップファイルは4つの各バックアップファイルグループごとにシステムにリストアすることができます。
ここでは例として[バックアップ手順の例]で設定を行った[システム設定のファイル]グループのファイルのバックアップファイルをシステムにリストアする際の操作手順の例を説明します。

1. Management Console画面左の[システム]アイコンをクリックする。

   [システム]画面が表示されます。

2. [システム]画面の[その他]一覧の[バックアップ/リストア]をクリックする。

   [バックアップ/リストア一覧]画面が表示されます。

3. 一覧の[システムの設定ファイル]の左側の[リストア]をクリックする。

   [リストア]画面が表示されます。

4. [リストア]画面で[バックアップのリストア先]、[バックアップ方式]、[リストアするバックアップファイル]を指定し、[リストア]をクリックする。

   通常は、デフォルトで最も新しいバックアップファイルが選択されています。そのまま実行すれば、最新のバックアップファイルがリストアされます。

   重要

   [元のディレクトリにリストアする]を選択した場合、現在のファイルの内容がバックアップしておいた内容で上書きされますので注意してください。

5. 「リストアします。よろしいですか?」というダイアログボックスが表示されます。リストアする場合は[OK]をクリックする。

   リストアをしない場合は、[キャンセル]をクリックしてください。

   ヒント

   選択したバックアップファイルの内容を参照したい場合は、[表示]をクリックしてください。